Авторизація з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем

Державна служба спеціального зв'язку та захисту інформації України

Основні зміни внесені Законом України №4336-IX

Закон України № 4336-IX від 27.03.2025 «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури»

- Закон України «Про Державну службу спеціального зв’язку та захисту інформації України»
- Закон України «Про основні засади забезпечення кібербезпеки України»
- Закон України «Про стандартизацію»
- Закон України «Про захист інформації в інформаційно-комунікаційних системах»

Нормативна база авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем

Закон України «Про захист інформації в інформаційно-комунікаційних системах»

Постанова Кабінету Міністрів України від 18 червня 2025 року № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем»

Базовий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація, затверджений наказом Адміністрації Держспецзв'язку від 30.06.2025 № 409

Базовий профіль безпеки системи, де обробляється службова інформація, затверджений наказом Адміністрації Держспецзв'язку від 02.07.2025 № 419

Базові профілі безпеки системи, де обробляється інформація, що становить державну таємницю з грифом обмеження доступу «Таємно» та «Цілком таємно» (за окремим запитом)

Наказ Адміністрації Держспецзв'язку від 11.07.2025 № 438 "Про затвердження Вимог до юридичних осіб, фізичних осіб — підприємців, які здійснюють оцінювання реалізації цільового профілю безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем", зареєстровано в Мін'юсті України 31 липня 2025 року за № 1125/44531

Наказ Адміністрації Держспецзв'язку від 11.07.2025 № 434 "Про затвердження Порядку ведення переліку авторизованих систем з безпеки", зареєстровано в Міністерстві юстиції України 01 серпня 2025 року за № 1140/44546

НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем»

Наказ Адміністрації Держспецзв'язку від 04.09.2025 № 545 " Про затвердження Порядку перевірки авторизаційної документації", зареєстровано в Мін'юсті України 19 вересня 2025 року за № 1361/44767

Наказ Адміністрації Держспецзв'язку від 08.12.2025 № 810 "Про затвердження Рекомендацій з оцінювання дотримання вимог цільового профілю безпеки системи"

Наказ Адміністрації Держспецзв'язку від 08.12.2025 № 811 " Про затвердження Рекомендацій з розроблення цільового профілю безпеки системи "

Наказ Адміністрації Держспецзв'язку від 17.12.2025 №836 "Про встановлення вимог щодо запровадження постачальниками заходів безпеки відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури", зареєстровано в Міністерстві юстиції України 31 грудня 2025 року за №№ 1975/45381–1978/45384

НД ТЗІ 2.3-025-24 Т1-Т3 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем)

Перехідний період від КСЗІ до авторизації з безпеки системи

 ІКС	Оцінена КСЗІ	Без модернізації до кінця терміну дії документу про оцінку відповідності	**Авторизації з безпеки системи після завершення терміну дії документу про оцінку відповідності**
 ІКС	Початок створення КСЗІ до 18.06.2025	Документ про відповідність до 18.06.2026 (Наказ Адміністрації Держспецзв'язку № 93)	**Авторизації з безпеки системи з 18.06.2026**
 ІКС	Початок створення КСЗІ на ІКС, що обробляє ДТ до 18.06.2025	Документ про відповідність на 12 місяців	**Авторизації з безпеки системи протягом 12 місяців з дня реєстрації атестата**
 ІКС	Початок створення КСЗІ по ПКМУ № 627 до 18.06.2025	Декларація, яка дійсна 3 роки	**Авторизації з безпеки системи після завершення терміну дії декларації**

Переваги перед КСЗІ

Основні переваги авторизації з безпеки перед КСЗІ:

Ризик-орієнтований підхід

Замість сліпого виконання всіх вимог стандартів (що часто робиться в КСЗІ), авторизація фокусується на оцінці реальних ризиків та впровадженні заходів, що захищають від конкретних загроз.

Гнучкість та швидкість

Замість створення складної системи з нуля, використовуються базові, галузеві або цільові профілі безпеки. Це значно пришвидшує процес впровадження захисту.

Адаптація до сучасних технологій

Авторизація краще підходить для сучасних хмарних сервісів, ІКТ-систем та швидкої модернізації, тоді як КСЗІ часто була прив'язана до фізичної інфраструктури.

Зменшення бюрократії

Авторизація діяльності замість тривалої експертизи КСЗІ знижує навантаження на бізнес та державу.

Постійний моніторинг

Авторизація передбачає безперервне підтримання безпеки, а не одноразову експертизу, яка застаріває відразу після отримання

Зміни до постанови КМУ від 29.03.2008 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем»

- Система повинна **обов’язково** виконувати технічні та організаційні вимоги до захисту та кіберзахисту, визначені Мінімальними вимогами

- Вимоги визначаються **базовим** або **галузевим** профілем безпеки, залежно від функціонального призначення системи
- Виконання Мінімальних вимог підтверджується:
  - **авторизацією системи з безпеки** — для всіх систем;
  - сертифікатом відповідності стандарту інформаційної безпеки, виданим органом з оцінки відповідності (крім систем, що обробляють державну таємницю).

Постанова КМУ від 18.06.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем»

Затверджує :

- Порядок авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем - визначає процедури проведення авторизації з безпеки;

- Порядок розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем - визначає механізм розроблення та затвердження базових, галузевих та цільових профілів безпеки.

Основні етапи авторизації з безпеки систем

I — Розроблення та затвердження для системи цільового профілю

II — Виконання вимог цільового профілю

III — Оцінювання дотримання вимог цільового профілю

IV — Оформлення та подання Адміністрації Держспецзв’язку авторизаційного листа

V — Внесення даних щодо авторизації до переліку авторизованих систем з безпеки

Порядок розроблення та затвердження профілів безпеки систем

Адміністрація Держспецзв’язку

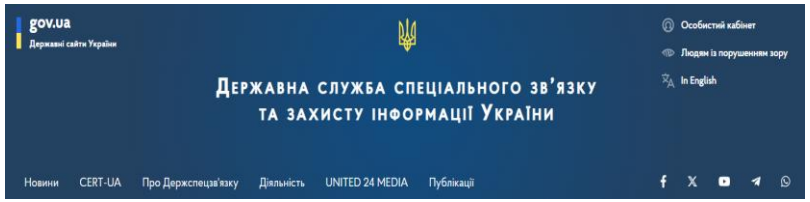
розробляє

затверджує

Базові профілі безпеки системи розробляються залежно від інформації, що обробляється у системі (відкрита інформація чи інформація з обмеженим доступом), а також функціонального призначення системи та затверджуються Адміністрацією Держспецзв’язку

переглядає

публікує на офіційному веб-сайті Держспецзв’язку базові профілі безпеки системи, які містять відкриту інформацію



Базові профілі безпеки

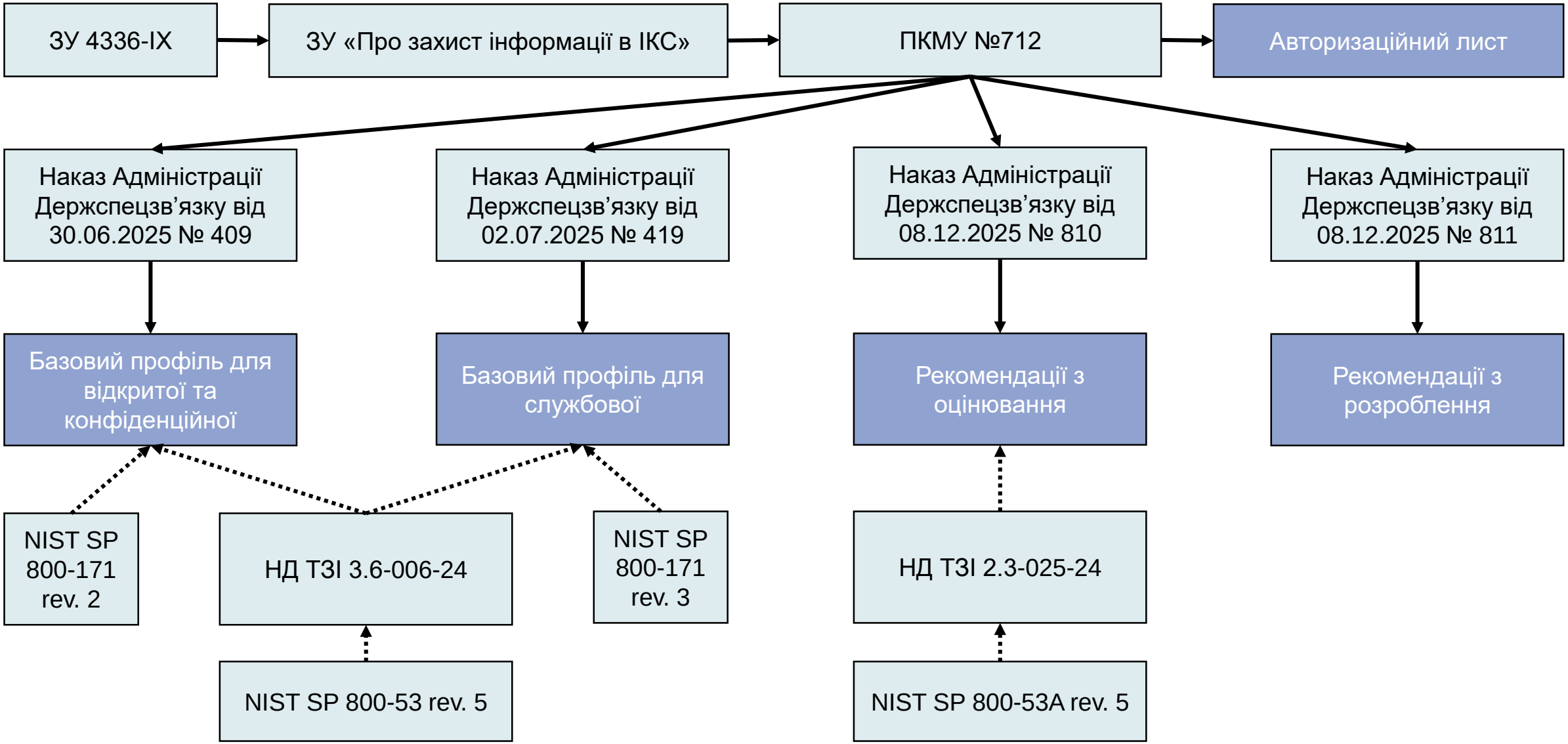
Базовий профіль безпеки для відкритої та конфіденційної
Базовий профіль безпеки для службової
Базовий профіль безпеки для таємної
Базовий профіль безпеки для цілком таємної

Галузеві профілі безпеки

Міністерство цифрової трансформації України
Міністерство оборони України
Міністерство енергетики України
Служба безпеки України

Кожні два роки здійснює перегляд вимог базового профілю безпеки системи та у разі необхідності вносить відповідні зміни

Логічний зв’язок нормативно-правових документів



Цільовий профіль безпеки (ЦПБ)

I

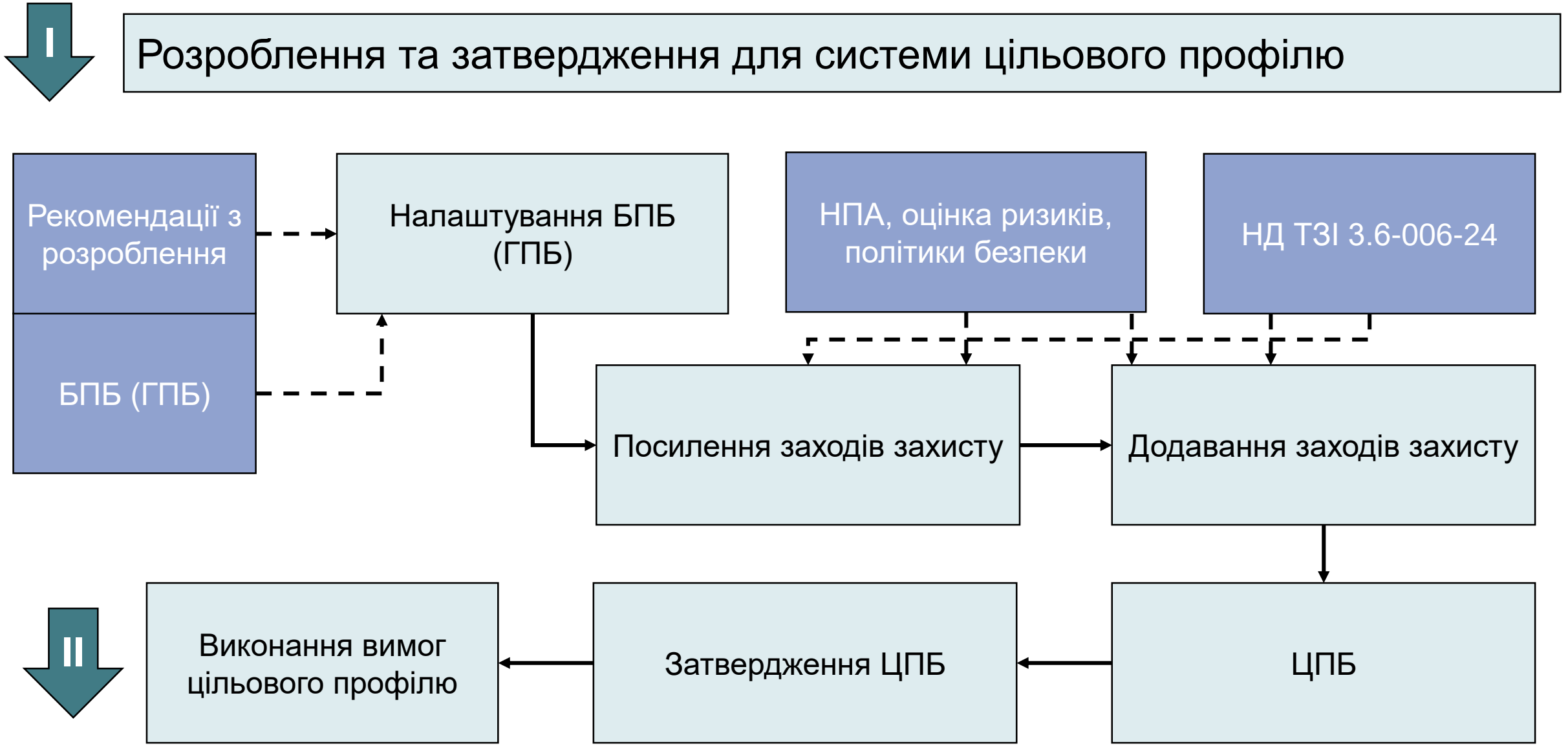
Розроблення та затвердження для системи цільового профілю

- Документ, що визначає конкретний перелік заходів захисту інформації для системи
- Формується на основі базового або галузевого профілю безпеки (БПБ / ГПБ)
- Ураховує вид інформації, обмеження доступу та функціональне призначення системи
- Базується на архітектурі системи та результатах оцінювання ризиків
- Є обов'язковим етапом авторизації системи з безпеки

Рекомендації з розроблення цільового профілю безпеки системи, затвердженні Наказом Адміністрації Держспецзв’язку від 08.12.2025 № 811

- Розроблені відповідно до ПКМУ №712.
- Застосовується під час авторизації систем з безпеки
- Поширюється на інформаційні, інформаційно-комунікаційні та технологічні системи

Розробка цільового профілю безпеки



Основні стандарти з оцінки ризиків

I

Розроблення та затвердження для системи цільового профілю

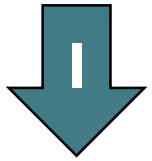
ДСТУ ISO/IEC 27005:2023 (Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки):

Стандарт надає рекомендації щодо впровадження процесу керування ризиками інформаційної безпеки в організаціях будь-якого типу та розміру.

NIST SP 800-30 Rev. 1 (Guide for Conducting Risk Assessments):

Настанова (guide) від Національного інституту стандартів і технологій США, яка описує методологію оцінки ризиків для інформаційних систем.

Практичне застосування та перегляд ЦПБ



Розроблення та затвердження для системи цільового профілю

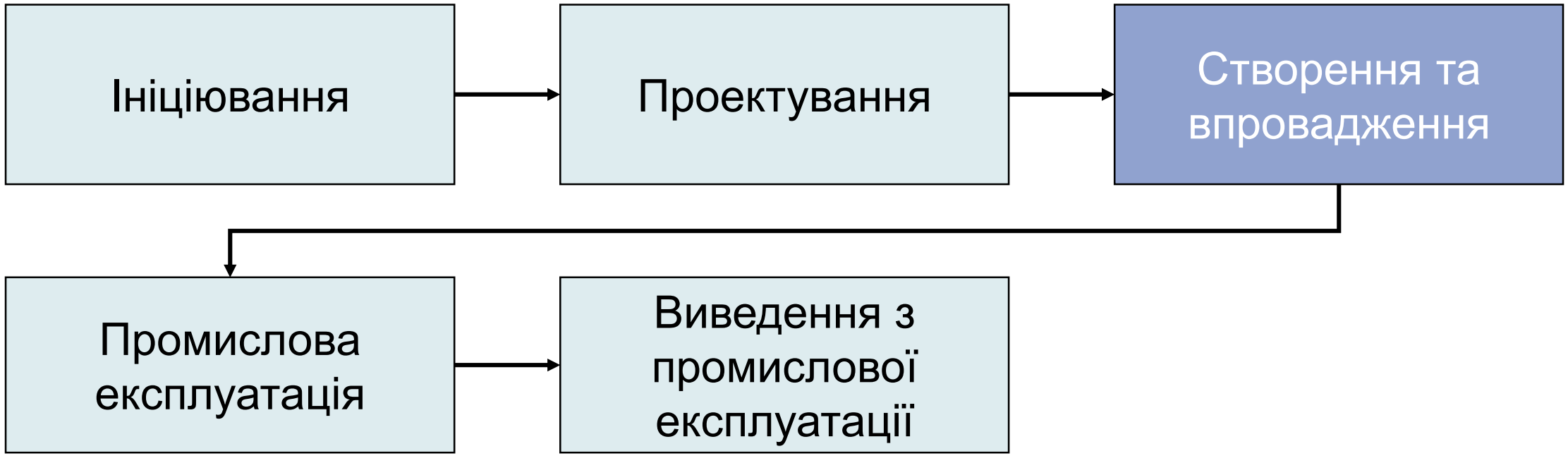
- Перегляд під час планової авторизації з безпеки
- Оновлення у разі зміни БПБ / ГПБ або результатів оцінки ризиків
- Перегляд при зміні архітектури або технології обробки інформації
- Можливість оформлення приміток у разі архітектурних обмежень

Постанова КМУ від 21 лютого 2025 року № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації»

II

Виконання вимог цільового профілю

Засіб інформатизаціїї протягом життєвого циклу проходить такі стадії



III

Оцінювання дотримання вимог цільового профілю

- **Постанова Кабінету Міністрів України від 31.12.2025 № 1799** «Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури»
- **Наказ Адміністрації Держспецзв’язку від 11.07.2025 № 438** "Про затвердження Вимог до юридичних осіб, фізичних осіб — підприємців, які здійснюють оцінювання реалізації цільового профілю безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем"

Для здійснення оцінювання захищеності інформації оцінювачі повинні мати один із документів, виданих Адміністрацією Держспецзв’язку:

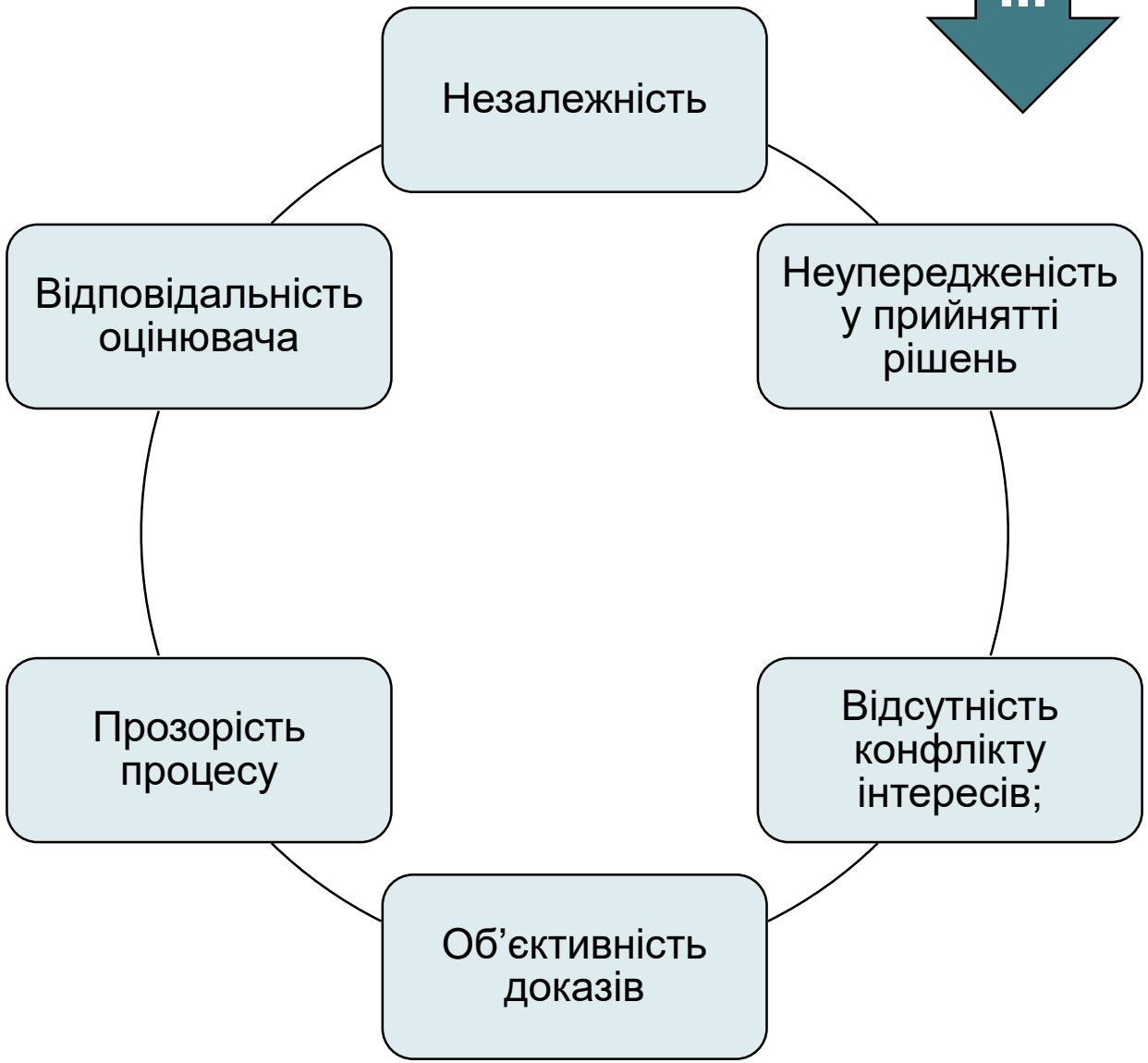
1. Ліцензію на провадження діяльності у сфері технічного захисту інформації за видами: оцінювання захищеності інформації, що не становить державної таємниці або оцінювання захищеності інформації усіх видів, у тому числі інформації, що становить державну таємницю.

2. Дозвіл на проведення робіт з технічного захисту інформації для власних потреб

Основні принципи оцінювання

III

Оцінювання дотримання вимог цільового профілю



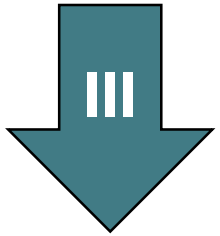
Рекомендації з оцінювання дотримання вимог цільового профілю безпеки системи, затвердженні Наказом Адміністрації Держспецзв’язку від 08.12.2025 № 810

III

Оцінювання дотримання вимог цільового профілю

- Розроблені відповідно до ПКМУ №712.
- Визначають рекомендований порядок оцінювання безпеки систем.
- Застосовуються під час авторизації системи з безпеки, внутрішніх і зовнішніх аудитів.
- Спрямовані на перевірку відповідності систем вимогам ЦПБ.

Процес оцінювання дотримання вимог ЦПБ

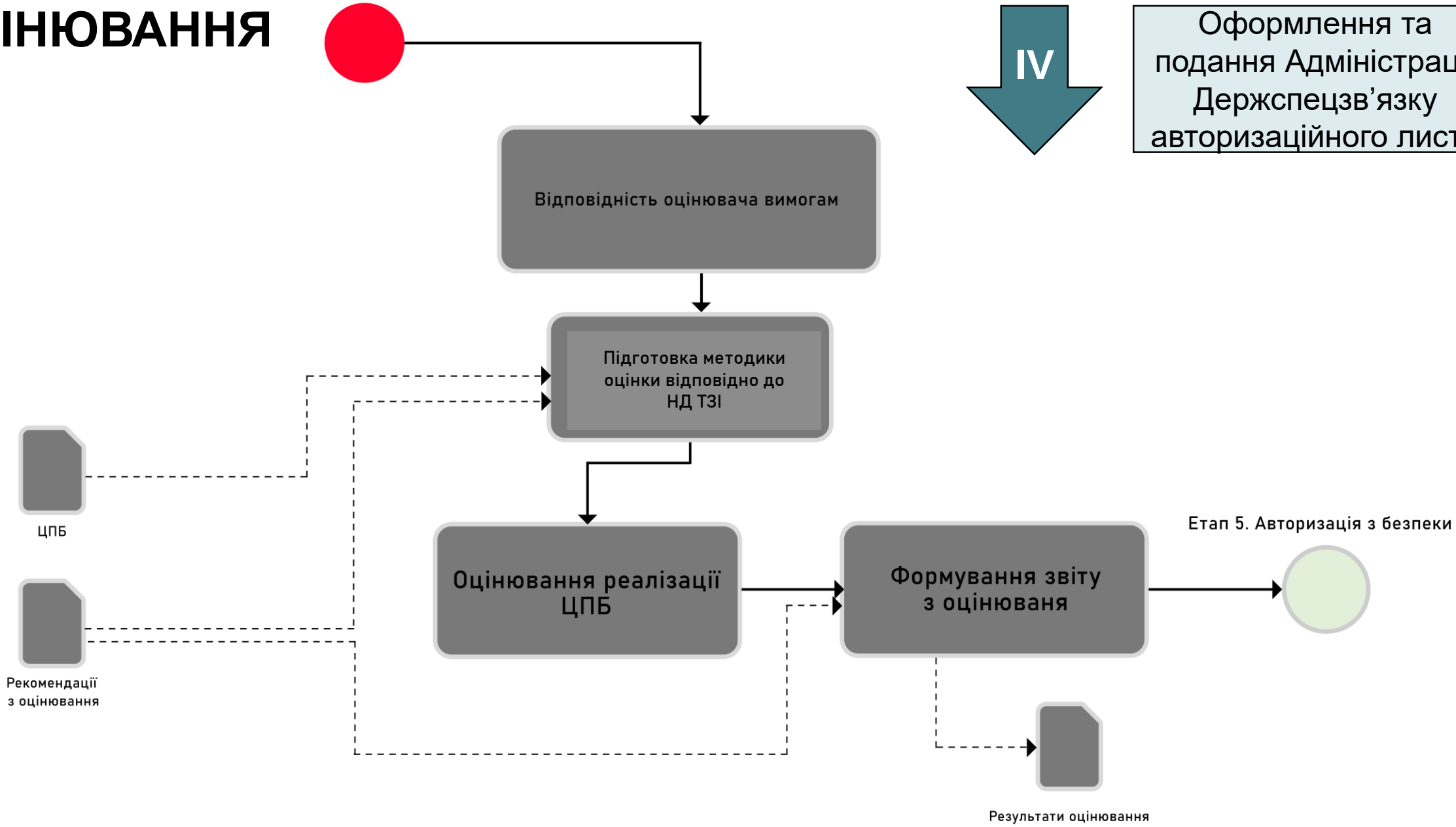


Оцінювання дотримання вимог цільового профілю

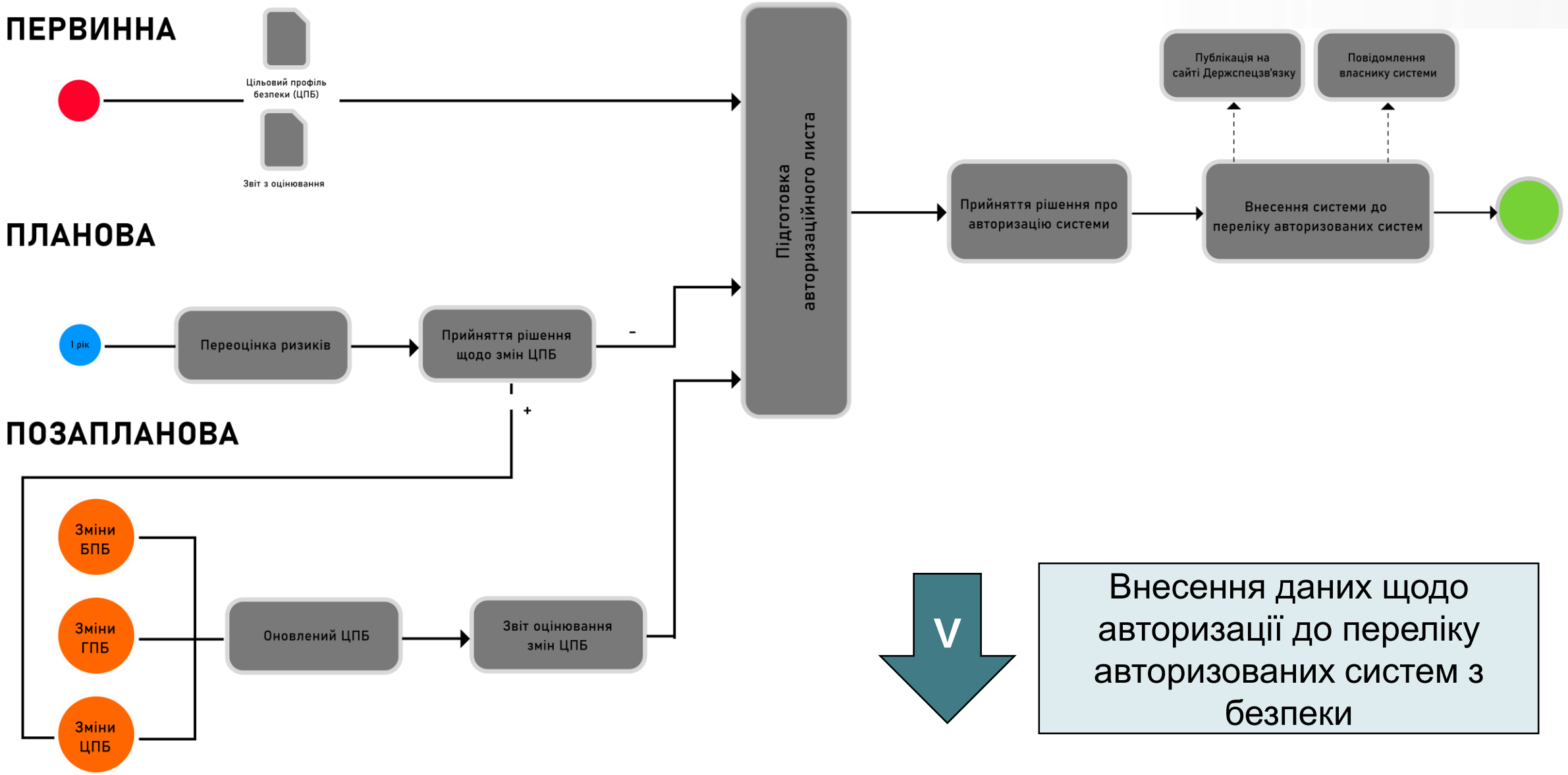
Оцінювання дотримання вимог ЦПБ включає такі етапи:

1. Оцінювання ЦПБ — перевірка коректності вибору базового або галузевого профілю безпеки та відповідності вимогам законодавства.
2. Оцінювання реалізації ЦПБ — перевірка фактичного впровадження заходів захисту, аналіз документації, механізмів і дій персоналу.
3. Оформлення результатів — підготовка звіту з доказами та загальними висновками.

ОЦІНЮВАННЯ


IV
Оформлення та подання Адміністрації Держспецзв’язку авторизаційного листа
Відповідність оцінювача вимогам
Підготовка методики оцінки відповідно до НД ТЗІ
ЦПБ
Рекомендації з оцінювання
Оцінювання реалізації ЦПБ
Формування звіту з оцінюваня
Етап 5. Авторизація з безпеки
Результати оцінювання

АВТОРИЗАЦІЯ



Внесення даних щодо авторизації до переліку авторизованих систем з безпеки

Скасування авторизації з безпеки систем

ПІДСТАВИ:

Подання до Адміністрації Держспецзв’язку письмового звернення власника або розпорядника системи про скасування авторизації з безпеки системи

Не проведення у встановлені строки планової авторизації з безпеки системи

Непроведення у встановлені строки позапланової авторизації з безпеки системи у випадках змін базового профілю або галузевого профілю, на основі якого був сформований цільовий профіль

Невиконання у встановлені строки вимог щодо усунення порушень, виявлених за результатами проведення державного контролю за додержанням вимог законодавства у сферах технічного та криптографічного захисту інформації, кіберзахисту

Рішення про скасування авторизації з безпеки системи приймається Адміністрацією Держспецзв’язку протягом 30 робочих днів після отримання відповідних відомостей

У разі скасування авторизації з безпеки системи наступне включення системи до переліку авторизованих систем з безпеки здійснюється як первинна авторизація з безпеки системи

Система управління інформаційною безпекою (СУІБ)

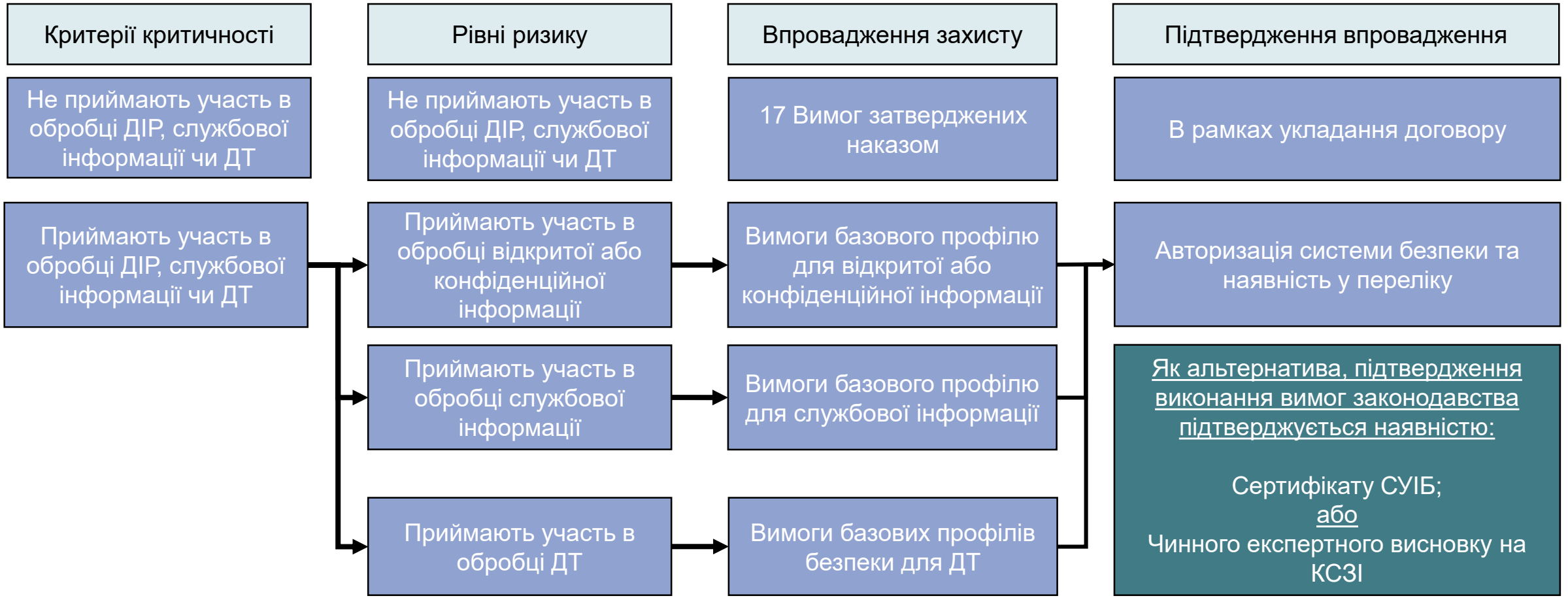
- Будується відповідно до ISO/IEC 27001
- Комплексний підхід до захисту інформаційних активів
- Управління ризиками, політики та процедури, технічні й організаційні заходи
- Підтверджується сертифікацією (крім систем з державною таємницею)
- Обов’язкове виконання вимог базових профілів безпеки

Ключові аспекти сертифікації ISO 27001:

- Термін дії: Сертифікат дійсний 3 роки з моменту видачі.
- Контрольна сертифікація (Наглядовий аудит): Проводиться щороку (на 2-й та 3-й роки) для підтвердження того, що система залишається ефективною та відповідає вимогам стандарту.
- Ресертифікація: Після закінчення 3-річного терміну проводиться повна повторна сертифікація.

Ключова ідея: цілісна система, що постійно вдосконалюється для забезпечення конфіденційності, цілісності та доступності інформації.

Наказ Адміністрації Держспецзв'язку від 17.12.2025 № 836 «Про встановлення вимог щодо запровадження постачальниками заходів безпеки відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури»



Алгоритм визначення постачальниками порядку дій

Державна служба спеціального зв'язку та захисту інформації України